

Werken volgens de Wet politiegegevens; een praktische handreiking voor boa's



1. Over dit document

Gemeenten in Nederland hebben in de loop der jaren steeds meer taken en verantwoordelijkheden gekregen, onder meer op het gebied van openbare orde en veiligheid. Deze uitbreiding van taken heeft ook geleid tot toenemende complexiteit in het werk van de buitengewoon opsporingsambtenaar (boa). Boa's fungeren steeds vaker als partners binnen netwerken en de strafrechtketen.

Om deze steeds complexere taken te kunnen blijven uitvoeren, hebben boa's door de jaren heen ook meer bevoegdheden gekregen. Om deze toegenomen bevoegdheden in evenwicht te brengen met privacybelangen, is in 2019 de Wet politiegegevens (Wpg) ook van toepassing geworden op het werk van boa's.

De Wpg brengt een reeks van verplichtingen met zich mee. Deze verplichten staan naast de regels van de Algemene Verordening Gegevensbescherming (AVG).

Dit document geeft uitleg over deze verplichtingen en hoe wij binnen de gemeente Oldebroek met deze verplichtingen omgaan. Deze werkinstructie fungeert als naslagwerk ter ondersteuning van het werk van de boa en als verduidelijking van taken voor de rest van de organisatie.

2. Inhoudsopgave

1. Over dit document
2. Inhoudsopgave
3. Voor en tijdens het verwerken van persoonsgegevens
 - 3.1 Welke systemen gebruikt de gemeente Oldebroek
 - 3.2 Proportionaliteit, noodzakelijkheid en subsidiariteit
 - 3.3 Onderscheid in verschillende grondslagen
 - 3.4 Artikel 8: dagelijkse opsporingstaak
 - 3.5 Artikel 9: gerichte verwerking

- 3.5.1 Wat te doen bij een artikel- 9-verwerking
- 3.6 Artikel 13: Ter ondersteuning van het werk
- 3.7 De Wpg en het proces-verbaal: onderscheid persoonlijke oordelen en feiten
- 3.8 Onderscheid tussen verschillende categorieën betrokkenen
- 3.9 Waarschuwing verwerken bijzondere persoonsgegevens
- 4. Archivering en bewaartermijnen in de context van de Wpg
 - 4.1 Bewaartermijn artikel 8: dagelijkse opsporingstaak
 - 4.2 Bewaartermijn artikel 9: gerichte verwerking
 - 4.3 Bewaartermijn artikel 13: Ter ondersteuning van het werk
- 5. Functioneel beheerder en boa-coördinator
 - 5.1 Goedkeuring en steekproeven
 - 5.2 Positie bij audits
 - 5.3 Aanspreekpunt NatuurNetwerk
 - 5.4 Beroep op recht van inzage
 - 5.5 Autorisaties
 - 5.6 Autorisatie niet-boa
 - 5.7 Periodieke DPIA
 - 5.8 Aanstellingsprocedure nieuwe boa
- 6. Ter beschikking stellen en verstrekken
 - 6.1 Ter beschikking stellen
 - 6.2 Verstrekken en verstrekkingenwijzer
 - 6.3 Onderscheid maken in de praktijk
 - 6.4 Onjuiste verstrekking
- 7. Rechten van betrokkenen
 - 7.1 Procedure gemeente Oldebroek
- 8. Bij binnenkomst
 - 8.1 Verzoek tot opsporingsbevoegdheid
 - 8.2 Aanwijzing als toezichthouder
 - 8.3 Toegang tot Brs
 - 8.4 Toegang tot eventuele andere systemen
- 9. DPIA in de context van Brs
 - 9.1 DPIA in algemene zin
 - 9.2 Brs
 - 9.3 DPIA in de H2O-gemeenten
- 10. Bijlagen
 - 10.1 Bijlage 1: Grip op privacy. Rechten van betrokkenen
 - 10.2 Bijlage 2: Stroomschema ter beschikking stellen of verstrekken

3. Voor en tijdens het verwerken van persoonsgegevens

3.1 Welke systemen gebruikt de gemeente Oldebroek

Binnen de gemeente Oldebroek vervullen de buitengewoon opsporingsambtenaren (boa's) binnen domein I twee hoofdfuncties: handhaver en toezichthouder. Afhankelijk van de specifieke functie bevinden zij zich in verschillende regimes bij het verwerken van persoonsgegevens.

Wanneer een boa persoonsgegevens verwerkt als toezichthouder, vallen deze gegevens onder de Algemene Verordening Gegevensbescherming (AVG). Als de boa persoonsgegevens verwerkt als handhaver, vallen deze onder de Wet politiegegevens (Wpg). Beide soorten persoonsgegevens hebben verschillende regels met betrekking tot gegevensbeheer, opslag, systemen en werkprocessen.

Het Boa Registratie Systeem (Brs) en het Toezichthouders Registratie Systeem (Trs) faciliteren het correct verwerken van persoonsgegevens volgens de geldende regels. Deze applicaties werken gedeeltelijk geautomatiseerd.

De richtlijn binnen de gemeente Oldebroek is dat het verwerken van persoonsgegevens in het kader van de Wpg altijd plaatsvindt binnen de omgeving van Brs. Het verwerken van persoonsgegevens in het kader van toezichthouderschap gebeurt op dit moment nog binnen het zaaksysteem Djuma, maar

op termijn hopen we over te kunnen gaan op TRS en zal het verwerken van persoonsgegevens in het kader van toezichthouderschap plaatsvinden binnen de context van Trs. Dit document fungeert primair als handleiding voor het wettelijk verwerken van persoonsgegevens die vallen onder de context van de Wpg.

3.2 Proportionaliteit, noodzakelijkheid en subsidiariteit

Voordat je over gaat tot het verwerken van de persoonsgegevens – of deze gegevens nu onder de Wpg of AVG vallen – is het zaak bij jezelf te raden te gaan of het verwerken van de persoonsgegevens te verantwoorden is. De standaard vragen die de boa hierbij behoort te wegen zijn:

- staat de verwerking in verhouding tot het doel dat je hebt (proportionaliteit);
- zijn alle gegevens daadwerkelijk noodzakelijk voor het te bereiken doel (noodzakelijkheid);
- kan het doel ook bereikt worden op een manier die minder inbreuk maakt op de privacy van de betrokkenen (subsidiariteit).

3.3 Onderscheid in verschillende grondslagen

Vallen de te verwerken persoonsgegevens binnen de context van het regime handhaving en is het verwerken van de persoonsgegevens te verantwoorden, dan is het nog van belang om te weten op welke grondslag van de Wpg de persoonsgegevens mogen worden verwerkt. Dit dient ook als zodanig te worden gemuteerd in Brs.

Bij het Besluit Politiegegevens Buitengewoon Opsporingsambtenaren is bepaald dat alleen de artikelen 8, 9 en 13 relevant zijn voor de boa als grondslag voor het verwerken van persoonsgegevens die vallen onder de Wpg.

3.4 Artikel 8: dagelijkse opsporingstaak

Persoonsgegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak, vallen onder artikel 8 van de Wpg. Dit gaat over zaken als wildplassen, foutief aanbieden van afval, alcohol gebruiken op de openbare weg en loslopende honden. Ook proces-verbaal opmaken bij onrechtmatig afgeschoten wild of tuinafvaldump vallen hieronder. De gegevens kunnen zowel over verdachten, slachtoffers als andere betrokkenen gaan.

In het werk van de boa zullen verreweg de meeste verwerkingen van politiegegevens binnen de grondslag van artikel 8 vallen.

3.5 Artikel 9: gerichte verwerking

Dit artikel maakt het mogelijk om gegevens te verwerken die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. De inbreuk op de privacy is bij deze verwerkingen groter dan bij artikel 8. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stropen of stelselmatige observatie bij verdenking van een milieudelict. Ook een gericht onderzoek naar het vergiftigen van vossen of dumping van asbest kan onder artikel 9 vallen, bijvoorbeeld als je verwacht dat het onderzoek langer dan veertig uur duurt of als er meerdere opsporingsambtenaren bij betrokken zijn.

Artikel 9-gegevens mogen worden verwerkt tot het doel bereikt is; dat weet je dus niet van tevoren. In de praktijk kun je zeggen: tot er een onherroepelijk vonnis is of tot de verjaringstermijn bereikt is. Daarom moet binnen een week het doel van de verwerking worden aangemeld op een door de boa-werkgever bepaalde werkwijze. Binnen de gemeente Oldebroek geeft de boa dit aan in Brs.

3.5.1 Wat te doen bij een artikel-9 verwerking

Omdat er bij artikel 9-verwerkingen meer inbreuk op de privacy van de betrokkenen te verwachten is, zijn in de wet extra waarborgen ingebouwd. Eén van deze waarborgen is dat elke artikel 9-verwerking een Bevoegd Functionaris moet hebben. Hij of zij is verantwoordelijk voor dat specifieke onderzoek en moet ervoor zorgen dat de privacy van de betrokkene niet onevenredig geschaad wordt. Daarom heeft de wetgever dus de bevoegd functionaris (BF) geïntroduceerd.

Voor veel kleinere boa-werkgevers is de last van het zelf in dienst hebben van een bevoegd functionaris disproportioneel zwaar. Dit geldt ook voor de gemeente Oldebroek. Daarom is er voor organisaties die gebruik maken van het BRS gekozen voor een pragmatische oplossing.

Het samenwerkingsverband waarin alle gebruikersorganisaties verenigd zijn (het SupBRS) heeft ervoor gekozen om BF's op te leiden en in te voeren in Brs. Iedere boa kan vervolgens, indien hij van mening is dat zijn verwerking onder het regime van artikel 9 dient plaats te vinden, een BF selecteren. Dit betekent dus dat je een BF kunt kiezen die werkzaam is bij een andere organisatie.

Voordat een artikel-9-traject wordt ingezet, is het de richtlijn binnen de gemeente Oldebroek om dit eerst te bespreken met de boa-coördinator binnen de organisatie.

Op het moment dat men besluit om een artikel 9-verwerking in gang te zetten is het wel van belang dat men snel handelt. De wet verplicht om binnen een week het doel van de verwerking vast te leggen. Dit gebeurt in samenspraak met de bevoegd functionaris. In het geval van de gemeente Oldebroek gebruiken wij een bevoegd functionaris afkomstig van het netwerk van BRS. Dit kan enige vertraging veroorzaken. Daarom is het van belang aan de voorkant snel in actie te komen.

In de werkzaamheden van de boa, zullen artikel-9-verwerkingen zeer zeldzaam zijn.

Soms kan het bepalen van de scheidslijn tussen de grondslagen uit artikel 8 en 9 van de Wpg lastig zijn. Op de website van Boa Registratie Systeem staat een nog uitgebreidere uitleg over het onderscheid tussen artikel 8 en 9. Onderstaande link gaat naar deze toelichting:

<https://www.natuurnetwerk.info/BRSdocumenten/Instructie%20scheidslijn%20artikel%208%20en%209%20v1.1.pdf>

Het document is ook opgenomen in de map Wpg-conform-werken.

3.6 Artikel 13: ter ondersteuning van het werk

Dit artikel biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9, vaak landelijk, verder te verwerken. De verwerkingsverantwoordelijke kan zelf een artikel-13- verwerking starten, nadat hij een bijbehorend artikel-13-protocol heeft opgesteld. De gegevens die onder artikel 13 verwerkt worden, komen voort uit artikel 8- of 9-verwerkingen. Bepaalde gegevens kunnen tegelijkertijd onder artikel 13 als onder 8 of 9 verwerkt worden.

Vooralsnog zijn er in heel Nederland nog geen artikel-13-verwerkingen voor boa's bekend.

3.7 De Wpg en het proces-verbaal: onderscheid persoonlijke oordelen en feiten

Voor het proces van eventuele strafvordering is het van belang dat een opsporingsambtenaar in zijn bevindingen onderscheid maakt tussen vaststaande feiten en persoonlijke oordelen. Voor het proces-verbaal in het bijzonder geldt dat daar het liefste alleen feiten in staan.

Waar dit in algemeenheid bekend is voor de boa, legt de Wpg hier nog eens extra de nadruk op in artikel 4, lid 3. Het artikel stelt: 'voor zover mogelijk worden politiegegevens die op feiten zijn gebaseerd onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd'.

Dit maakt daarom, dat ook voor de Wpg geldt dat het belangrijk is dat elk proces-verbaal in beginsel gebaseerd is op feiten. Hier worden namelijk de nodige conclusies uit getrokken.

Derhalve is het aan te bevelen om voor ogen te houden geen meningen of conclusies vast te leggen. Zaken zoals:

- Ik zag dat hij dronken was
- Ik zag dat hij sliep
- Ik zag dat hij mij boos aankeek
- Ik zag dat hij woedend weg liep
- Ik zag dat hij mij wilde slaan

zijn allemaal meningen of conclusies. Het is de opsporingsambtenaar niet toegestaan om die in een proces-verbaal op te nemen.

Als je denkt dat iemand ligt te slapen in een portiek, zou je de volgende feiten kunnen vermelden: *Ik zag dat daar een man lag met gesloten ogen. Ik hoorde dat hij een snurkend geluid maakte. Ik schudde stevig aan de arm van deze man en ik riep: 'wakker worden'.*

Ik zag dat die man zijn ogen opende. Ik hoorde en zag dat hij zei: 'Wat is er, wie maakt mij wakker?'

Als dat van belang is, dan bepalen anderen aan de hand van jouw waarnemingen wel of deze man sliep.

De functioneel beheerder zal sporadisch de juistheid van het proces-verbaal controleren. Dit punt wordt verder toegelicht in hoofdstuk 5.1; "goedkeuring en steekproeven functioneel beheerder".

3.8 Onderscheid tussen verschillende categorieën betrokkenen

Een volgend element om Wpg-conform te werken, is het maken van onderscheid tussen verschillende categorieën van betrokkenen bij het verwerken van politiegegevens. Hierbij gaat het onder andere om het noteren van bevindingen bij het opmaken van het proces-verbaal.

De meest voorkomende categorieën van betrokkenen zijn:

- verdachten;
- slachtoffers (benadeelden);
- derden (zoals getuigen).

Dit betreft echter geen absoluut onderscheid omdat een verdachte gedurende het opsporingsonderzoek tot getuige kan transformeren en andersom.

3.9 Waarschuwing verwerken bijzondere persoonsgegevens

Niet alle persoonsgegevens zijn hetzelfde. Sommige persoonsgegevens die in de context van de Wpg verwerkt kunnen worden vallen onder de categorie bijzondere persoonsgegevens. Verwerking van deze categorie persoonsgegevens is in beginsel verboden. Bij de wet is bepaald dat persoonsgegevens waaruit het volgende blijkt vallen onder de categorie bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- gegevens over gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Wees dus ook terughoudend bij het gebruik van beeldmateriaal. Een foto van een persoon bevat mogelijk informatie over zijn ras en wellicht zijn er meer bijzondere gegevens uit af te leiden, zoals de religie op basis van de gedragen kleding.

Ondanks het verbod laat de wetgever een enkele opening voor het verwerken van dit soort persoonsgegevens. Het verbod geldt, tenzij dit onvermijdelijk is voor het doel van de verwerking en in aanvulling op de verwerking van andere politiegegevens.

Mocht je als boa binnen de gemeente Oldebroek genoodzaakt zijn om bijzondere persoonsgegevens te verwerken, dan is het de richtlijn om dit bespreekbaar te maken met de boa-coördinator. Het liefste gebeurt dit voor het verwerken van deze persoonsgegevens, maar dit kan ook achteraf als de situatie geen andere mogelijkheid biedt.

4. Archivering en bewaartermijnen in de context van de Wpg

Zoals al in het vorige hoofdstuk naar voren is gekomen, bevat de Wpg drie artikelen die de basis vormen voor boa's bij het verwerken van politiegegevens. Dit zijn de artikelen 8, 9 en 13. Deze verschillende grondslagen bepalen niet alleen het toegestane doel van de verwerking, maar ook de bewaartermijnen. Deze termijnen variëren per artikel.

Voor de gemeente Oldebroek geldt dat we werken met Brs. Brs ontzorgt onze organisatie. Het programma houdt zelf de verschillende bewaartermijnen in de gaten. Nadat de bewaartermijn is verstreken, worden de gegevens automatisch in 'de kluis' geplaatst of verwijderd.

Ondanks deze automatisering is het belangrijk dat de boa en de functioneel beheerder zelf ook alert blijven met betrekking tot het handhaven van de bewaartermijnen.

4.1 Bewaartermijn artikel 8: dagelijkse opsporingstaak

Artikel 8-gegevens mogen tot vijf jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd en verwerkt. Bijvoorbeeld door te zoeken op een naam, adres of kenteken. Daarna worden ze vijf jaar bewaard (bewaartermijn) en daarna dienen ze te worden vernietigd. Gedurende de bewaartermijn kunnen de gegevens gebruikt worden voor het afhandelen van klachten en voor audits of een controle door de Autoriteit Persoonsgegevens. Verder geldt dat deze gegevens onder bepaalde omstandigheden ter beschikking kunnen worden gesteld voor hernieuwde verwerking. Ze komen dan als het ware opnieuw tot leven in een actueel opsporingsonderzoek. Gegevens in de bewaartermijn mogen ook verwerkt worden voor wetenschappelijk onderzoek en statistiek.

4.2 Bewaartermijn artikel 9: gerichte verwerking

Artikel 9-gegevens mogen worden verwerkt tot het doel bereikt is; dat weet je dus niet van tevoren. In de praktijk kun je zeggen: tot er een onherroepelijk vonnis is of tot de verjaringstermijn bereikt is. Daarom moet binnen een week het doel van de verwerking worden aangemeld op een door de boa-werkgever bepaalde werkwijze. Is het doel bereikt, dan heeft de bevoegd functionaris (BF) nog zes maanden de tijd om informatie uit het onderzoek aan te bieden aan collega's die deze kunnen hergebruiken voor hun eigen onderzoek. Daarna worden ze vijf jaar bewaard en daarna dienen ze te worden

vernietigd. Gedurende de bewaartermijn kunnen de gegevens voor dezelfde doeleinden worden gebruikt als de bewaarde gegevens uit artikel 8.

4.3 Bewaartermijn artikel 13: Ter ondersteuning van het werk

Gegevens die verder verwerkt worden onder artikel 13, worden aan het einde van hun verwerkingstermijn niet eerst verwijderd, maar direct vernietigd. Wanneer dit moet gebeuren, dient te blijken uit het bij die verwerking behorende artikel 13-protocol. Deze termijn wordt door de verwerkingsverantwoordelijke bepaald en gemotiveerd en verschilt dus per artikel 13-verwerking.

De termijnen voor specifieke artikel 13-verwerkingen zijn terug te vinden in de betreffende protocollen en in het verwerkingsregister binnen de omgeving van Brs.

5. Functioneel beheerder en boa-coördinator

Binnen de gemeente Oldebroek is de keuze gemaakt om te werken met een functioneel beheerder naast de boa-coördinator. De functioneel beheerder is onderdeel van het boa-team en vormt het eerste aanspreekpunt voor vragen over het gebruik van Brs en samen met de boa-coördinator aanspreekpunt voor vragen over de Wpg.

5.1 Goedkeuring en steekproeven

Binnen Brs moet elk proces-verbaal goedgekeurd worden door de functioneel beheerder voordat deze wordt opgestuurd naar het Centraal Justitieel Incassobureau. De richtlijn binnen de gemeente Oldebroek is dat de functioneel beheerder dit bij goed vertrouwen doet. Hij of zij zal niet elk proces-verbaal inhoudelijk beoordelen.

Daarentegen voert de functioneel beheerder periodiek steekproeven uit om de inhoudelijke en procedurele juistheid van de processen-verbaal te controleren. De richtlijn is dat vier processen-verbaal per twee maanden willekeurig worden beoordeeld. De bevoegd functionaris is het toegestaan hier bij eigen discretie van af te wijken.

5.2 Positie bij audits

Zowel de functioneel beheerder als de boa-coördinator hebben een praktische taak bij audits. Hij of zij ondersteunen bij het aanleveren van de noodzakelijke informatie en documentatie voor het uitvoeren van de audit.

De Wpg stelt dat er twee varianten van audits moeten worden uitgevoerd naar de omgang met politiegegevens binnen de organisatie. Elk jaar vindt een interne audit plaats door de functionaris gegevensbescherming. Elke vier jaar vindt een externe audit plaats naar de naleving van de Wpg. Deze externe audit wordt uitgevoerd door een externe partij.

Voor beide audits geldt dat er bewijsstukken moeten worden aangeleverd. Deze bewijsstukken moeten bij elkaar worden gezocht en worden overgedragen aan functionaris gegevensbescherming. Dit is een gezamenlijke taak van de functioneel beheerder en de boa-coördinator. Samen hebben zij het meeste zicht op de werkvloer, waar de feitelijke verwerking van politiegegevens plaatsvindt.

De functioneel beheerder, boa-coördinator en de functionaris gegevensbescherming onderhouden contact met elkaar over het goed en tijdig verlopen van de audit.

5.3 Aanspreekpunt NatuurNetwerk

De functioneel beheerder fungeert als contactpersoon tussen het NatuurNetwerk-platform en de gemeente (en vice versa). Als er vragen zijn vanuit één van de organisaties of vanuit het gebruikersplatform (SupBRS), dient de functioneel beheerder als doorgeefluik. Daarnaast houdt deze persoon (de functioneel beheerder van de gemeente) zicht op nieuwe gebruikersmogelijkheden voor Brs en Trs.

5.4 Beroep op recht van inzage

Onder de Wpg hebben betrokkenen recht van inzage in de door de gemeente verwerkte politiegegevens die over hen gaan. Wat aanleiding geeft tot deze rechten staat beschreven in het hoofdstuk 7, "Rechten van betrokkenen". Hoe de procedure tot het geven van inzage er precies uitziet staat beschreven onder bijlage 1 in het document "Grip op privacy. Rechten van betrokkenen".

Bij het verlenen van inzage speelt de functioneel beheerder een belangrijke rol binnen de gemeente Oldebroek. Deze functioneert als aanspreekpunt voor H2O Privacy.

Op het moment dat een verzoek tot inzage binnenkomt, komt deze in de eerste instantie terecht bij de privacy officer van H2O. Deze persoon zal in de meeste gevallen de beoordeling van het verzoek doen. Zo nodig voor de beslissing, zal de privacy officer contact opnemen met de gemeente om samen tot

een besluit te komen. Hierin treedt de functioneel beheerder op als contactpersoon tussen gemeente en privacy officer.

Wordt het verzoek goedgekeurd door de privacy officer, dan komt deze persoon op de lijn bij de functioneel beheerder van de gemeente Oldebroek. De privacy officer zal bij de functioneel beheerder het verzoek neerleggen de benodigde acties te nemen die vereist zijn om het recht door te voeren. De functioneel beheerder stuurt eventueel de noodzakelijke documentatie door naar de privacy officer. Daarbij wordt (bij een standaard verzoek) een termijn van 5 werkdagen gehanteerd.

De privacy officer voorziet vervolgens in het contact met de aanvrager (betrokkene) en levert eventueel ook de noodzakelijke documentatie aan deze persoon.

De regel vanuit H2O Privacy is om het gehele verzoek binnen één maand te voorzien van een reactie. Als het verzoek complex is of indien blijkt dat bij verschillende regionale eenheden of bij de landelijke eenheid van de politie politiegegevens over de verzoeker worden verwerkt, kan dit met 6 weken worden verlengd. In dit geval moet de verzoeker binnen de initiële maand geïnformeerd worden over de verlengde termijn en de reden voor deze vertraging. Dit wordt geregeld en op toegezien door H2O Privacy.

5.5 Autorisaties

Een andere functie van zowel de functioneel beheerder als van de boa-coördinator is het regelen van autorisaties en het toezicht houden op verleende autorisaties.

De verschillende programma's/applicaties die binnen de gemeente Oldebroek gebruikt worden door het boa-team bevatten veel gevoelige informatie. Om deze informatie veilig te houden is het belangrijk dat er controle bestaat op wie deze informatie kan inzien. Daarom werken deze programma's/applicaties met een autorisatieprocedure. Dit geldt onder andere ook voor BRS.

Wanneer iemand toegang wil tot de inhoud van deze programma's, verloopt dit via de functioneel beheerder en de boa-coördinator. Deze houden naar eigen inzicht toezicht op welke personen, welke vormen van autorisatie hebben binnen de programma's en applicaties. Bij het beoordelen of een autorisatie gewenst is, wordt rekening gehouden met de wettelijke regels en de beginselen van proportionaliteit, noodzakelijkheid en subsidiariteit. Een persoon krijgt enkel toegang op het moment dat dit strikt noodzakelijk is voor zijn of haar functie.

In het kader van toezicht op autorisaties bekijken en beoordelen de functioneel beheerder en boa-coördinator met enige regelmaat welke personen binnen de organisatie waartoe geautoriseerd zijn. De frequentie waarmee dit toezicht plaatsvindt is naar eigen beoordeling, maar vindt minstens twee maal per jaar plaats.

5.6 Autorisatie niet-boa

In bepaalde gevallen is het wenselijk om niet-boa's te autoriseren om specifieke gegevens in te kunnen zien. Hier gaat het om collega's binnen de gemeente die bijvoorbeeld toegang nodig hebben voor bepaalde administratieve werkzaamheden. Ook kan het zijn dat zij toegang nodig hebben voor het analyseren van opsporingsgegevens.

De wet staat het toe deze mensen (tijdelijk) te autoriseren. Hiervoor moet wel een verklaring worden getekend. Deze verklaring moet ondertekend worden door een manager om rechtsgeldig te zijn. Op deze manier blijft de werkgever verantwoordelijk. De functioneel beheerder ondersteunt in het invullen van de verklaring.

Onderstaande link leidt naar een modelverklaring van Boa Registratie Systeem:
[BRS modelverklaring autorisatie niet boa BRS 2020 v1.1.pdf \(natuurnetwerk.info\)](#).

Het document is ook opgenomen in de map Wpg-conform-werken.

5.7 Periodieke DPIA

Op het moment dat een organisatie voornemens is een grote, impactvolle en/of structurele verwerking van persoonsgegevens door te voeren, moet een DPIA worden uitgevoerd. Een DPIA is een schriftelijk onderzoeks- en legitimeringsdocument, die de houdbaarheid van een bepaalde verwerking toetst.

Bij de introductie is een dergelijke DPIA uitgevoerd op de impact van BRS. Hiermee is de kous echter niet af. Elke drie jaar moet de DPIA opnieuw uitgevoerd worden.

Hierin bekleedt de boa-coördinator een belangrijke rol. De boa-coördinator is formeel de proceseigenaar bij het uitvoeren van de DPIA. Hij of zij neemt in het jaar dat de laatste DPIA drie jaar geleden heeft

plaatsgevonden het initiatief door een privacy officer van H2O privacy te contacteren. De boa-coördinator en de privacy office maken samen afspraken over hoe de DPIA uitgevoerd gaat worden en wie daar eventueel nog meer bij betrokken dient te worden.

Meer informatie over de DPIA staat vermeld in hoofdstuk 9, *"DPIA in de context van Brs en Trs"*.

5.8 Aanstellingsprocedure nieuwe boa

Een laatste taak die belegd moet worden is het organiseren van de aanstellingsprocedure bij het in dienst treden van een nieuwe boa binnen het cluster toezicht en handhaving.

Deze procedure bestaat uit een aantal onderdelen. Hierbij gaat het om:

- Het verzoek doen tot opsporingsbevoegdheid en alles wat daarmee samenhangt, zoals onder andere de beëdiging van de nieuwe boa;
- Het aanwijzen van de nieuwe boa als toezichthouder;
- De nieuwe boa van toegang voorzien tot Brs;
- De nieuwe boa van toegang voorzien tot eventuele andere systemen die hij of zij nodig heeft voor het uitvoeren van het werk.

Deze door de functioneel beheerder en boa-coördinator uit te voeren handelingen, staan nader toegelicht in hoofdstuk 8, *"Bij binnenkomst"*.

6. Ter beschikking stellen en verstrekken

Een boa kan op twee manieren zijn of haar politiegegevens delen met anderen. Bij de ene manier gaat het om het ter beschikking stellen van de gegevens met anderen binnen het wpg-domein. Dit gaat vrij gemakkelijk. Bij de andere manier gaat het om het verstrekken van politiegegevens aan anderen buiten het Wpg-domein. Dit proces is meer complex en is sterk aan voorwaarden onderworpen.

6.1 Ter beschikking stellen

Ter beschikking stellen is het delen van politiegegevens binnen het Wpg-domein. Dit is beschreven in artikel 15 van de Wpg. Een synoniem hiervoor is 'free flow of information'. In principe dienen politiegegevens gedeeld te worden met ieder die de gegevens nodig heeft voor de uitoefening van zijn of haar taak. Bij dit 'need to know'-principe hoort altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt.

Het delen van gegevens die onder de Wpg vallen binnen het Wpg-domein is dus aan relatief weinig aanvullende regels gebonden. De organisaties die binnen dit domein vallen, zijn:

- De politie;
- De Koninklijke Marechaussee;
- Andere buitengewoon opsporingsambtenaren;
- De vier bijzondere opsporingsdiensten (BOD'en).

6.2 Verstrekken en verstrekkingenwijzer

In de Wpg is vastgelegd aan welke partijen buiten het Wpg-domein je gegevens mag verstrekken. Voor elke verstrekking geldt dat deze moet worden geadmistreerd. Dit omdat als een betrokkene om inzage vraagt, hij moet kunnen zien met wie zijn gegevens gedeeld zijn. In de verstrekkingenwijzer voor boa's is uitgewerkt aan wie verstrekt mag worden en wat de voorwaarden zijn. In gevallen waarbij structureel gegevens verstrekt worden, is het bijvoorbeeld noodzakelijk dat hier een convenant aan ten grondslag ligt en dat hiertoe zwaarwegende belangen spelen (zoals genoemd in artikel 20 Wpg).

De verstrekkingenwijzer is een omvangrijk bestand. Daarom is er voor gekozen deze niet op te nemen in dit document, maar er naar te verwijzen met een externe link: [Verstrekkingenwijzer Wpg voor boa v1.6.pdf \(natuurnetwerk.info\)](#). Eveneens is dit document opgenomen in de map "Wpg-conform-werken".

6.3 Onderscheid maken in de praktijk

Soms kan het lastig zijn om te bepalen of er sprake is van ter beschikking stellen of van verstrekken van politiegegevens. Om hierin te ondersteunen is er een stroomschema beschikbaar. Dit stroomschema is opgenomen onder bijlage 2.

6.4 Onjuiste verstrekking

Bij het delen van persoonsgegevens gelden zorgvuldigheid en discretie als basisprincipes. Dit is voor persoonsgegevens die onder de Wpg vallen niet anders. Daarom is het ook van substantieel belang dat wanneer de stap tot verstrekken wordt gezet, enkel de juiste gegevens worden verstrekt. Evenzeer is het van groot belang dat de verstrekte gegevens allen terecht komen bij de bedoelde partij en dat deze partij alleen de strikt noodzakelijke politiegegevens ontvangt.

Mocht dit verkeerd gaan en zijn er onjuiste gegevens verstrekt of zijn deze aan een verkeerde organisatie verstrekt, dan is het belangrijk dat hier snel op geacteerd wordt. De wet stelt dat de benadeelde partij zo spoedig mogelijk geïnformeerd moet worden en dat de foutieve persoonsgegevens moeten worden geïdentificeerd en vervolgens gerectificeerd. Voor de gemeente Oldebroek is de afspraak gemaakt dat iedereen in cluster toezicht en handhaving die een onjuiste verstrekking ontdekt dit direct bespreekbaar maakt in het team. Vervolgens wordt onmiddellijk contact opgenomen met een privacy officer van H2O privacy.

Samen met de privacy officer worden vervolgens afspraken gemaakt om tot een oplossing te komen. De privacy officer kan hierin ook contact opnemen met de afdelingsmanager van de afdeling Ruimte van de gemeente.

7. Rechten van betrokkenen

Een belangrijke overweging om de regels rond het gebruik van politiegegevens aan te scherpen in 2019, is het beter beschermen van de privacy van betrokkenen. Onderdeel hiervan is dat betrokkenen de mogelijkheid krijgen beter inzicht te krijgen in de verwerking van hun gegevens. Daarom hebben mensen van wie wij als gemeente persoonsgegevens hebben verwerkt het recht om deze in te zien.

Door hen inzage te verlenen kunnen zij zicht krijgen op welke gegevens de gemeente precies van hen heeft verwerkt. Ook biedt dit hen de mogelijkheid te controleren of de gegevens die over hen verwerkt worden, juist, volledig, ter zake dienend en noodzakelijk zijn. Als dat niet zo is, dan hebben zij nog een aantal rechten. Zo kunnen zij vragen om aanpassing, verwijdering en afscherming van gegevens die op hen betrekking hebben.

7.1 Procedure gemeente Oldebroek

Betrokkenen kunnen hierover informatie vinden in de privacyverklaring op de website van de gemeente Oldebroek. Hier worden hun rechten toegelicht en kunnen zij ook lezen hoe zij een afspraak kunnen maken voor een moment van inzage.

Hoe dit proces daarna voor de organisatie precies verloopt, is vastgesteld in het H2O-document *“Grip op privacy. Rechten van betrokkenen”*. Dit document staat onder bijlage 1. Ook wordt in hoofdstuk 5, *“Functioneel beheerder en boa-coördinator”* het procedureel verloop binnen het team Ruimte van de gemeente Oldebroek specifiek beschreven.

In dit document staat ook vernoemd onder welke voorwaarden inzage verleend mag worden. In de praktijk zijn er slechts enkele redenen om een kennisnemingsverzoek te weigeren: bijvoorbeeld als de veiligheid van de staat in gevaar komt, of als het leidt tot schending van de rechten van anderen. Maar in vrijwel alle gevallen zal er inzage moeten worden gegeven.

8. Bij binnenkomst

Op het moment dat een nieuwe boa in dienst treedt bij de gemeente Oldebroek moet er veel geregeld worden. Zo moet de nieuwe boa beschikken over een uniform, een steekwerend vest en een telefoon. Deze zaken zijn tastbaar en duidelijk, maar misschien nog belangrijker zijn de administratieve aangelegenheden die tijdig geregeld moeten worden. Dit omdat deze aanvraagprocedures vaak meerdere weken duren. Door aanvragen op tijd in te dienen, kan de nieuwe collega zo snel mogelijk de straat op.

In het hele proces van het indienstreden spelen de functioneel beheerder en boa-coördinator een centrale rol in het organiseren en aanvragen.

8.1 Verzoek tot opsporingsbevoegdheid

Het verzoek doen tot opsporingsbevoegdheid heeft bij het aanstellen van een nieuwe boa prioriteit. Dit omdat deze aanvraag tot 13 weken in beslag nemen kan. De boa-coördinator dient dit verzoek in bij Justis.

Voor de gemeente Oldebroek begint de procedure met het invullen en opsturen van het formulier: *“Aanvraag-/Mutatieformulier - Individuele buitengewoon opsporingsambtenaar (boa)”*. Dit document dient in zijn volledigheid te worden ingevuld. Hierbij is het belangrijk dat ook de juiste bijlagen worden bijgevoegd. Het gaat hierbij onder andere om bewijs van bekwaamheid, een actuele VOG P en een pasfoto (een volledige lijst van de noodzakelijke documentatie is te vinden op de website Justis).

Het formulier met bijlagen wordt vervolgens opgestuurd naar de direct toezichthouder (korpschef van de Nationale Politie). De direct toezichthouder brengt advies uit en stuurt dit advies op naar de toezichthouder (het openbaar ministerie). De toezichthouder stuurt vervolgens beide adviezen, plus de nood-

zakelijke bijlagen terug naar de gemeente (boa-coördinator). De gemeente stuurt dit hele pakket aan documentatie op haar beurt op naar Justis.

Van Justis ontvangt de gemeente vervolgens bericht over het goed- of afkeuren van het verzoek. Wanneer het verzoek is goedgekeurd ontvangt men in hetzelfde bericht van Justis een uitnodiging met een tijd en locatie voor de beëdiging van de nieuwe boa. Vaak zal dit op het politiebureau van Apeldoorn zijn. Tijdens deze afspraak legt de nieuwe boa ook de eed of belofte af voor zijn functie als buitengewoon opsporingsambtenaar en committeert hij zich effectief aan de geheimhoudingsplicht die komt met dit ambt.

Mocht het zo zijn dat het verzoek wordt afgewezen, dan geeft Justis in de afwijzing aan waar dit aan ligt. Daarna heeft men een aantal weken om de fout te herstellen. De boa-coördinator neemt ook in het herstellen van het verzoek het initiatief. Zo nodig verzameld de boa-coördinator zelf de juiste mensen om zich heen om het probleem op te lossen.

8.2 Aanwijzing als toezichthouder

Naast buitengewoon opsporingsambtenaar zijn de boa's binnen de gemeente Oldebroek ook benoemt als toezichthouder, als bedoeld in artikel 5:11 Algemene wet bestuursrecht. Het toezichthouderschap is voor het kunnen handhaven binnen de gemeente net zo belangrijk als het verkrijgen van de opsporingsbevoegdheid.

Om als toezichthouder aan de slag te gaan, moet deze persoon aangewezen zijn als toezichthouder door het bestuursorgaan dat de toezichthouder als zodanig kan aanwijzen. Ook heeft de boa een toezichthouderspas nodig.

Het aanwijzen als toezichthouder en het verzorgen van de toezichthouderspas wordt binnen de gemeente Oldebroek geregeld door de boa-coördinator.

8.3 Toegang tot Brs

Voor het adequaat aan de slag kunnen is het van belang dat de nieuwe boa toegang krijgt tot Brs. De gemeente Oldebroek heeft de keuze gemaakt om alle mutaties, processen-verbaal of anderzijds verslaglegging in het kader van de Wpg op te stellen in deze applicatie van NatuurNetwerk. Deze applicatie ondersteunt de boa's om conform de Wpg te werken.

De functioneel beheerder is verantwoordelijk voor de autorisaties binnen Brs. Dit geldt ook voor de autorisatie van een nieuwe Boa. De functioneel beheerder maakt een account aan voor de nieuwe boa en geeft deze de juiste autorisatie binnen de omgeving. Zo nodig neemt de functioneel beheerder ook contact op met NatuurNetwerk om het nieuwe account te verifiëren.

8.4 Toegang tot eventuele andere systemen

Naast Brs en Trs gebruikt de gemeente Oldebroek ook andere systemen. Dit bijvoorbeeld voor het ontvangen en afhandelen van meldingen. Het is eveneens belangrijk dat ook hiertoe de nieuwe boa bij binnenkomst toegang krijgt.

Het behoort tot de taken van de functioneel beheerder en boa-coördinator om er zorg voor te dragen dat dit geregeld is. Dit wordt gefaciliteerd door contact op te nemen met de Key user van het bewuste programma en de gewenste autorisatie door te geven.

Waar het regelen van de autorisaties primair de verantwoordelijkheid is voor de bevoegd functionaris, is het ook belangrijk dat de nieuwe boa zelf initiatief neemt. Mocht deze in zijn werkzaamheden bepaalde beperkingen tegenkomen, dan is het van belang dat dit tijdig kenbaar wordt gemaakt bij de functioneel beheerder.

9. DPIA in de context van Brs

9.1 DPIA in algemene zin

Een Data Protection Impact Assessment (DPIA) is een schriftelijk onderzoeks- en legitimeringsdocument. Een verwerker van persoonsgegevens moet een DPIA uitvoeren op het moment dat deze van plan is persoonsgegevens te verwerken, waarvan hij redelijkerwijs kan inschatten dat deze verwerking een hoog privacyrisico oplevert.

Het instrument dient om de wenselijkheid en juridische houdbaarheid van bepaalde (soorten) verwerkingen te controleren en administratief te motiveren. In een DPIA worden onder andere noodzaak, proportionaliteit en eventuele privacy risico's afgewogen. Ook worden de maatregelen beschreven die de gegevensverantwoordelijke treft om de rechten en vrijheden van natuurlijke personen zo goed mo-

gelijk te beschermen. Een DPIA heeft zodoende als doel om de organisatie actief een afweging te laten maken en gelijktijdig te laten zien dat zij conform de wet handelt.

Een Data protection impact assessment wordt een gegevensbeschermingseffectbeoordeling genoemd in het Nederlands.

Er zijn drie wetten die het uitvoeren van een DPIA verplichten. Dit zijn de:

- Algemene verordening gegevensbescherming (AVG);
- Wet politiegegevens (Wpg);
- Wet justitiële en strafvorderlijke gegevens (Wjsg).

Voor boa's van gemeenten geldt dat zij van deze wetten enkel te maken hebben met de AVG en de Wpg.

Bij welke vormen van verwerkingen een DPIA moet worden uitgevoerd staat omschreven onder artikel 35 van de AVG. De Europese privacytoezichthouders hebben uit het verdrag een lijst van 9 criteria geïsoleerd. Op het moment dat het waarschijnlijk is dat een verwerking van persoonsgegevens aan twee of meer criteria "voldoet", is het de vuistregel dat een DPIA moet worden uitgevoerd. De criteria zijn als volgt:

- Evaluatie of scoretoekenning;
- Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
- Stelselmatige monitoring;
- Gevoelige gegevens of gegevens van zeer persoonlijke aard;
- Op grote schaal verwerkte gegevens;
- Matching of samenvoeging van datasets;
- Gegevens met betrekking tot kwetsbare betrokkenen;
- Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen;
- De situatie waarin als gevolg van de verwerking zelf "betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst".

Ondanks deze criteria, staat het niet in steen geschreven wanneer een DPIA moet worden uitgevoerd. Organisaties zijn zelf verantwoordelijk voor het maken van de inschatting. Dit gaat zeker op voor de Wpg. De Wpg kent geen expliciete criteria voor wanneer een DPIA moet worden uitgevoerd. Deze wet kent enkel de verplichting tot het uitvoeren van het onderzoek en stelt dat dit moet gebeuren bij een mogelijk privacyrisico ten gevolge van een verwerking. In de praktijk gebruiken we ook voor de Wpg de criteria zoals deze gelden voor de AVG.

9.2 BRS

Waar een DPIA behoort te worden uitgevoerd voor het verwerken van persoonsgegevens, is het gelijktijdig een proces dat nooit helemaal af is. Dit geldt in het bijzonder voor het op grotere schaal verwerken van persoonsgegevens in digitale systemen. Dit brengt extra gevoeligheden met zich mee. Daarom raadt de Autoriteit Persoonsgegevens aan om voor dit soort systemen eens in de drie jaar een herhaling uit te voeren van de DPIA. Dit is dus drie jaar na het uitvoeren van de initiële DPIA tijdens het aanschafproces van het systeem.

Ook moet bij fundamentele veranderingen aan het programma of bij het wezenlijk anders gaan gebruiken van het programma het proces van de DPIA opnieuw uitgevoerd worden.

Brs is een dergelijk digitaal systeem. Daarom is de keuze gemaakt in de gemeente Oldebroek om eens in de drie jaar een DPIA uit te voeren voor de systemen van NatuurNetwerk.

Het uitvoeren van deze periodieke DPIA is een taak van de boa-coördinator. Dit zoals eerder benoemd is in hoofdstuk 5, "*Functioneel beheerder en boa-coördinator*".

9.3 DPIA in H2O-gemeenten

Binnen H2O-gemeenten zijn afspraken gemaakt over het uitvoeren van een DPIA.

De proceseigenaar voert in de basis de DPIA uit. Deze persoon heeft vaak het beste zicht op de praktijktoepassing van het systeem. In het geval van Brs is dit de boa-coördinator.

De proceseigenaar houdt de kalender in de gaten en plant ergens in het jaar een nieuwe DPIA. Dit is dus drie jaar na het uitvoeren van de laatste DPIA. Het uitvoeren van de DPIA gaat in samenwerking met H2O privacy.

De boa-coördinator overlegt met de privacy officer van H2O privacy welke personen eventueel verder ingeschakeld moeten worden voor hun expertise. Dit kan bijvoorbeeld iemand zijn van de ICT-afdeling. De privacy officer en de boa-coördinator plannen eveneens de verdere uitvoering van proces in.

Bij het uitvoeren van de DPIA maken de organisaties binnen H2O privacy gebruik van een vast format. Dit format staat op de website van de H2O-gemeenten en is te vinden middels onderstaande link: [leeg DPIA Format H2O - Intranet H2O \(h2o-samenwerking.nl\)](#).

10. Bijlagen

10.1 Bijlage 1: Grip op privacy. Rechten van betrokkenen

Procesbeschrijving

Alle stappen die worden genomen, dienen te worden bijgehouden binnen het Zaaksysteem door de privacy officer. De privacy officer kan de Functionaris Gegevensbescherming om advies vragen gedurende het proces.

Stap 1	Ontvangst verzoek De betrokkene doet een schriftelijk of mondeling verzoek tot inzage, wijziging, verwijdering, beperking, bezwaar en/of overdracht (dataportabiliteit) van zijn persoonsgegevens. Schriftelijke verzoeken Deze komen binnen via centraal mailadres, e-formulier of post. Alle verzoeken worden geregistreerd door DIV en krijgt een zaak binnen het Zaaksysteem waarbij de privacy officer wordt vastgesteld als behandelaar. Mondelinge verzoeken Een betrokkene kan mondeling een verzoek indienen aan de balie/loket/KCC. De baliemedewerker of een medewerker naar wie wordt gevraagd, maakt een ontvangstnotitie aan waarbij de soort persoonsregistratie, welke het betreft (bijvoorbeeld een aanvraag om vergunning of ingediend bezwaar) en de naam, geboortedatum en identificatie van betrokkene. Deze verzoeken worden vervolgens afgehandeld als een schriftelijk verzoek. e-Diensten/e-formulier Wanneer een inzage wordt afgehandeld via e-Diensten worden meerdere stappen automatisch ondersteund. Het gaat om het ontvangen en verwerken van de aanvraag, en identificatie.
Stap 2	Beoordeling verzoek en identificatie De privacy officer beoordeelt of er aandachtspunten zijn op basis van het verzoek. De privacy officer beoordeelt het verzoek om te bepalen wie de betrokken procesverantwoordelijke(n) is/zijn. Als het verzoek niet duidelijk is, bijvoorbeeld welke persoonsregistratie het betreft of op welk recht een beroep wordt gedaan, dan wordt om een verduidelijking gevraagd bij de indiener. De identiteit van de betrokkene moet worden vastgesteld. Uitgangspunt hierbij is dat de identiteit wordt vastgesteld op de minst vergaande manier. Doel is dat de verwerkingsverantwoordelijke geen twijfel heeft over de identiteit van betrokkene. Indien aanvullende informatie vereist is, wordt dit opgevraagd middels stap 3.
A	Beoordeling verzoek Indien nodig wordt samen met de betrokken procesverantwoordelijke(n) een beoordeling gemaakt van de volgende punten: • Is het verzoek duidelijk en welke persoonsregistratie(s) betreft het? • Waar wordt om gevraagd? • Wie is nodig om aan het verzoek te kunnen voldoen (intern binnen of buiten het proces, een externe verwerker of een externe verwerkersverantwoordelijke).
B	Identificatie <i>Indiener is onbekend</i> De indiener toont aan wie hij/zij is:

	• Middels de DigiD optie via de website. Het inzageverzoek komt digitaal binnen bij de gemeente waarbij middels login via DigiD is voldaan aan de identificatie. • Door een kopie van een ID op/mee te sturen, die als kopie kenbaar gemaakt mag zijn en waarbij het BSN onleesbaar gemaakt mag zijn. De naam, geboortedatum en het nummer van het ID-bewijs worden vastgelegd in de betreffende zaak. De kopie ID wordt meteen daarna vernietigd. • Indien geen kopie van een ID bij de eerste aanvraag is ontvangen, dan wordt door de behandelaar hierom schriftelijk gevraagd. Vermeld wordt hierbij dat zonder ID het verzoek niet in behandeling wordt genomen. • Door zich persoonlijk aan de balie van het hoofdkantoor te identificeren met een legitimatiebewijs. Daarbij worden naam, geboortedatum en het nummer van het ID-bewijs vastgelegd. • Indien de verzoeker geen kopie ID wil toezenden, dan kan met de gemeente waarin de verzoeker woont een afspraak worden gemaakt ter identificatie op locatie. <i>Indiener is bekend</i> Als de indiener bekend is binnen de gemeente en dit is aantoonbaar degene die het verzoek heeft ingediend, kan besloten worden om af te zien van identificeren. Deze actie c.q. beoordeling wordt uitgevoerd door de privacy officer eventueel in overleg met de betreffende procesverantwoordelijke.
Stap 3	Ontvangst bevestigen De betrokkene ontvangt per post een ontvangstbevestiging binnen drie werkdagen. **Indien nodig wordt men om verduidelijking/identificatie gevraagd.
Stap 4	Behandeling van het verzoek De privacy officer doet een verzoek bij de betrokken procesverantwoordelijke(n) om de benodigde acties te nemen die vereist zijn om het recht door te voeren. Daarbij wordt (bij een standaard verzoek) een termijn van 5 werkdagen gehanteerd. Bij grote en/of complexe verzoeken zal in overleg met de procesverantwoordelijke(n) een termijn bepaald worden. Op basis van de reikwijdte en de genomen stappen verzameld de privacy officer de bijbehorende resultaten/bewijsmateriaal.
Stap 5	Besluit op verzoek Op basis van de inhoudelijke behandeling van het verzoek wordt de betrokkene geïnformeerd en eventuele resultaten gedeeld.

10.2 Bijlage 2: Stroomschema ter beschikking stellen of verstrekken

